2026 年 11 月 25 日 – 11 月 26 日 · 日报

攻破银行密码所需核心量子门首次跌破十亿次

49 篇 · 16 个来源 | PDF | 本期汇总免费阅读

本 期 目 录

今日三件事
硬件前沿
算法与软件
产业与生态
学术前沿
今日影响
编辑点评

收录报道	49
信息来源	16
阅读时长	约 17 分钟

当 前 S O T A

物理比特	1, 180
2Q 保真度	99. 99%
逻辑比特	**96 LQ**

01 亮点

今日三件事



1 **RSA破译门槛首破十亿** 研究人员将破解RSA-2048公钥所需的量子资源首次压缩至10亿次托佛利门（三比特受控非门）以内[22]——击穿密码破译算力门槛，倒逼全球金融后量子迁移。

2 **欧盟拟设五百亿欧主权基金** 欧盟委员会发布《欧洲量子法案》提案，拟设规模达500亿欧元（约合3800亿元人民币）的主权科技股权基金[27][49]——创全球量子公共资本单笔纪录，筑牢欧洲全产业链壁垒。

3 **罗罗联手量子企业攻坚航发** 世外桃源、罗尔斯·罗伊斯与超威半导体在力克斯超算上跑通迄今最

大航空量子仿真工作流[20]——打通量子模拟在顶级航发工业落地的全流程工程验证。

02 硬件

硬件前沿



自旋量子计算

在硅基自旋量子比特测试中，研究人员采用CORPSE（补偿自旋激发引起的共振偏差脉冲）复合脉冲使单比特门保真度达到99.97%，并证实BIR-4（绝热宽带反转脉冲）在长达10天（240小时）内无需重新校准，旋转角度漂移严格维持在0.3度以内[23]。其免校准稳定时长较此前2至4小时即需停机重校的常态提升了约50倍；99.97%的单比特保真度已追平迪拉克（Diraq）在1开尔文温区创下的99.85%等同类SOTA基准，但在双比特门保真度上，距离澳大利亚硅量子计算公司（SQC）原子精度施主比特的99.99%及格芯代工300毫米晶圆抽测的99%两比特SOTA仍缺乏多比特联合测试数据；同时自旋路线在五大路线中操作数（N_ops仅10^2–10^3量级）垫底，多量子点紧密排布下的微波串扰与

密集读出扩展性仍是核心短板。该进展大幅减轻了稀释制冷机测控系统的算力开销，为英特尔、迪拉克等依托工业半导体产线推进自旋芯片扩展扫清了控制漂移阻碍。

拓扑量子计算

荷兰代尔夫特量子技术研究中心（QuTech）在《自然》发表成果，利用半导体-超导纳米线混合结构中诱导的马约拉纳准粒子（具备非阿贝尔统计特性的拓扑激发态），首次完成了拓扑物理量子比特的原型操控[35]。这是全球首个获得实验证实的马约拉纳拓扑比特，实现了从凝聚态物理假说到可控器件原型的跨越；但目前仅完成单比特概念验证，尚未开展拓扑编织（交换粒子轨迹执行逻辑门）的双比特门操作；横向对照超导路线谷歌Willow芯片达到的Λ≈2.1纠错压制因子及离子阱量子公司（Quantinuum）实现的48个全纠错逻辑量子比特，拓扑路线成熟度落后主流成熟路线至少5至8年，距离实用化仍缺乏可扩展编织与稳定读出证据。该突破为微软等长期布局拓扑路线的机构注入了信心，但短期内难以撼动超导与离子阱在商业算力市场的主导地位。

离子阱量子计算

离子量子（IonQ）宣布与英国剑桥大学深化战略合作，计划于2027年夏季前在剑桥部署一台256物理比特的离子阱量子计算机整机[18]。若按期交付，其标称物理比特数将达到目前商用全连通离子阱SOTA系统（量子公司98物理比特的Helios系统）的2.6倍；但该承诺目前属于商业意向通报（证据等级

E5），离子阱系统的固有瓶颈在于离子穿梭输运延迟（IT-02开销）与毫秒级较慢门时，若在256比特阵列上无法维持超过99.921%的全比特对两比特门保真度，累积通信延迟将严重制约算法效率。该合作巩固了英国在欧洲的量子算力承载力，加剧了IonQ与Quantinuum在整机部署订单上的直接竞争。此外，离子量子联合多伦多大学启动网络化离子阱攻关，探索利用光子互连实现多芯片分布式扩展[11]。

中性原子量子计算

科研人员在《物理评论快报》发表论文，展示了一种将量子信息编码于原子空间几何位置的新型测量型计算平台，并在二维晶格中制备出包含123个量子比特的纠缠原子网络[6]。该方案利用空间几何位置编码规避了单原子微波寻址的串扰阻碍，刷新了测量型空间编码架构的纠缠比特数纪录；但横向对比中性原子公开SOTA（原子计算公司Atom Computing的1180物理比特阵列，以及科埃拉QuEra实现的448物理比特/96逻辑比特系统），其网络规模落后头部近一个数量级，且中性原子平台固有的1至10赫兹极低循环重复率（S-09硬约束）和中路无损读出测量开销（NA-04）在此项工作中仍未解决。同日，另一团队利用里德堡中性原子处理器结合混合算法模拟了强关联二维费米-哈伯德系统，验证了中性原子模拟机在未纠错条件下的物理优势[32]。

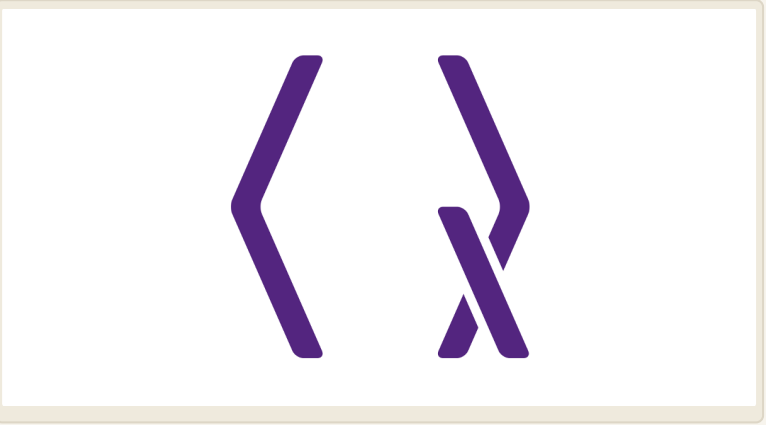
光量子与量子通信

实验团队研制出紧凑型集成化纠缠光子源，实现了每秒超过424万对的偏振纠缠光子产生速率，偏振可见度达99.6%[21]。其可见度追平了PsiQuantum在格芯300毫米晶圆上的99.50%不可分辨性基准，但该数据未披露包含片上耦合与探测在内的端到端损耗预算表（不满足PH-01红线），所有保真度均属于条件保真度，在缺乏系统级效率验证前无法折算为通用容错算力。清华大学团队在北京市城域商用光纤线路上实现单原子间纠缠分发速率达到546赫兹，较此前数十赫兹的纪录提升逾10倍，但距分布式计算所需的兆赫兹级互联仍差3个数量级[25]。此外，学者开发出双自由度超纠缠量子密钥分发方案，使单光子对承载2比特密钥[33]；马里兰大学提出利用商用光纤元件构建合成维度模拟高维多体物理的低成本方案[5]。

超导量子计算

继此前公布全球交付计划后，IQM量子计算公司正式签约韩国数据中心基础设施企业，将在首尔数据中心部署一台完整的IQM Radiance R3型54物理比特超导量子计算机整机[44][49]。该系统两比特门保真度处于超导商业中位水平（对标IBM Heron r2的99.5%基准），但整体规模与纠错能力距离谷歌Willow芯片展现的105比特、低于阈值纠错闭环仍有显著代差，依然属于NISQ（含噪声中等规模量子）硬件。该订单标志着超导整机进驻亚太商业数据中心，为极低温制冷机与量子测控机柜进入商业机房提供了标杆范本。

算法与软件



量子算法与资源优化

科研团队在最新资源估算研究中证实，通过重构模乘逻辑电路与流水线优化，将分解2048位RSA公钥（RSA-2048）所需的量子核心开销首次压缩至10亿次托佛利门（三比特受控非门）以内[22]。相较此前学界普遍估算的数十亿至上百亿次托佛利门开销，实现了资源需求数倍的大幅压缩，击穿了攻击实用公钥密码的核心操作门槛；但该指标建立在完美逻辑比特假设上，若按表面码千倍物理比特开销折算，仍需数百万物理比特支撑。该进展对银行密码与区块链安全构成长期实质威胁，将原本预估15年以上的密码淘汰期压缩至10年以内，倒逼金融机构加快抗量子密码迁移。此外，学者提出多项式函数对数深度量子态制备算法，将电路深度从线性O(n)压缩至对数O(log n)，攻克了量子化学仿真中的输入态编码瓶颈[16]。

编译器与自动化设计

新型形式化验证编译器QBlue正式推出，在哈密顿量（系统总能量算符）时间演化模拟电路的编译测试中，相较主流开源软件佩妮巷（PennyLane）实现了最高达94%的量子门数量削减[19]。该工具首次将数学定理证明与编译器优化统一，在百分之百杜绝浮点逻辑近似错误的前提下大幅压减门深度，使新药与新材料分子模拟能在更短相干时间内跑通。在版图工程端，自动化多模态智能体框架QlayBot在从拓扑图像生成二维芯片版图的测试中取得81.5%的一次性成功率，将原本耗时数天的版图绘制流程压缩至分钟级，消除了硬件流片的人力瓶颈[31]。

纠错架构与解码器

量子X实验室（Quantum X Labs）宣布其基于英伟达CUDA-Q纠错平台研发的QXL实时解码器，在谷歌超导量子硬件上实现了比标准最小权重完美匹配算法低12%至13%的逻辑错误率[24]。这证实了利用通用异构算力加速复杂图解码的可行性，仅凭软件优化即可压低一成以上逻辑失效率，推动专用解码加速卡成为量子测控系统的核心配置。针对非相干泄漏难题，研究人员提出层状表面码（Foliated surface codes）架构，在0.5%单步泄漏概率下将每两轮纠错周期的泄漏误差抑制了1380倍，为超导芯片向更大码距表面码演进扫除了能级跃迁障碍[29]。此外，学者提出递归克利福德噪声缩减方案（CliNR），以轻量开销压制克利福德电路逻辑错误[17]；体系结构学者提出的Schism动态互联调度

架构，在32个量子处理单元间实现了较固定拓扑4.9至7.3倍的芯片间通信加速[28]。

04 产业

产业与生态



主权资本与顶层政策

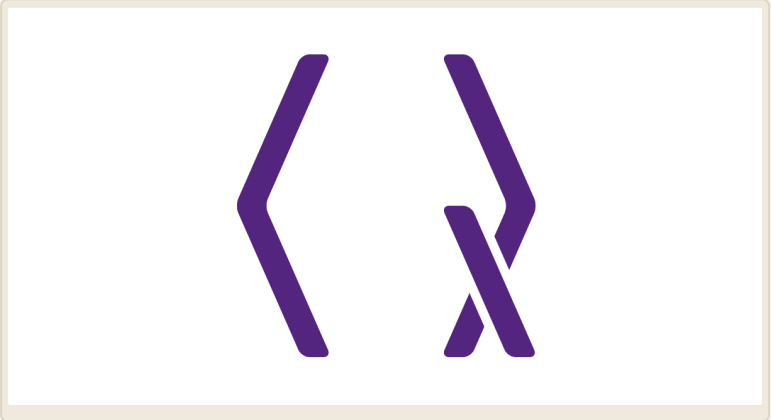
欧盟委员会正式推出《欧洲量子法案》法规提案，拟设立目标规模达500亿欧元（约合3800亿元人民币）的主权科技股权基金（STEF），欧洲量子产业联盟（QuIC）随即表态全力动员产业界对接落地[27][45][49]。这是全球迄今规模最大的主权科技股权投资计划，标志着欧洲扶持重点从学术实验室资助全面转向关键产业链自主可控与企业股权投资，显著增强了欧洲初创硬件厂商抵御美资并购的资本护城河。在美国，能源部副部长达里奥·吉尔（Darío Gil）披露创世纪任务实施首年已立项开展297个联合攻坚项目，旨在十年内使全美研发的生产力与影响力翻倍[1]；国会山听证专家组则警告，长寿命数据已面临量子威胁，老旧硬件的滞后正拖慢后量子密码防御部署，敦促联邦加速换代[3]。此外，泰国

朱拉隆功大学学者呼吁政府加强量子专业人才培养与研究支持，防范未来的产业与安全脱节[47]。

商业订单与跨界落地

世外桃源（Xanadu）、航空发动机巨头罗尔斯·罗伊斯与超威半导体（AMD）在力克斯（Lux）超级计算机上借助佩妮巷平台，成功跑通了面向下一代航空航天设计的超大规模量子仿真计算工作流[20]。该合作验证了高端重工业对混合量子算力的刚性需求，开创了芯片巨头、量子算法平台与顶尖制造企业三方协同的商业闭环，加速了航空重工将量子模拟整合至研发产线的进程。耐克森特资本（Nexent Capital）在阿布扎比设立ADGM一期封闭式基金，首期目标募集10亿美元（硬顶16亿美元），专项投向支持量子计算对接的高性能算力基础设施与先进能源，体现了中东主权资本将量子未来算力与低碳电网深度绑定的重资产投资逻辑[30]。渣打银行宣布在新加坡金融管理局支持下圆满结束首年技术验证，正式启动量子计算第二阶段扩建，加速算法在资产对冲与反洗钱中的落地[48]。行业调研报告则指出，当前量子化学与生命科学的早期商业化形态主要为混合软件平台与研发插件，短期内仍集中于软件授权与算力服务分成[2]。

学术前沿



凝聚态物理与分子仿真

由来自中国科研机构的十人团队凭借在国产百亿亿次超级计算机上实现的固氮酶铁钼辅因子（FeMo-co）超高精度量子模拟成果，正式荣获2026年度国际计算机协会戈登·贝尔奖[26]。团队利用先进数值算法攻克了困扰化学界数十年的强关联电子结构求解难题，计算精度完全达到此前理论预测必须依赖容错量子计算机方可达到的水平，大幅拉高了量子路线证明实用优越性的经典算力基准线。在模型仿真方面，学者在《量子》期刊展示了利用隧道耦合一维玻色气体冷原子系统模拟相对论正弦-戈登模型，观测到了场弛豫与拓扑相位锁定[14]；《自然·量子信息》刊发论文，利用区域注意力机制构建了开放系统长时演化算法，攻克了开放量子动力学环境退相干的维度爆炸瓶颈[4]。

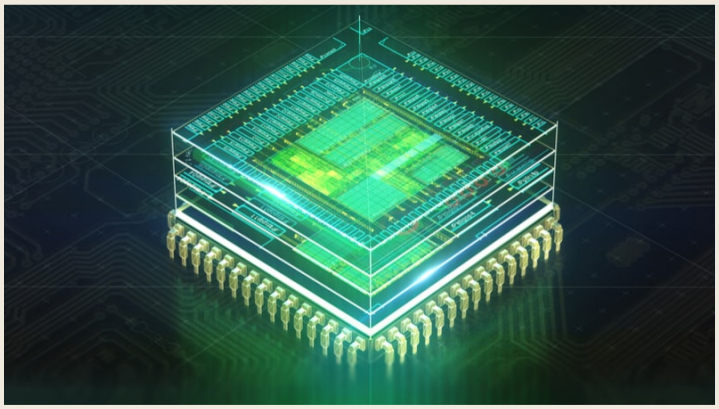
基础计算理论与度量

理论复杂性学者斯科特·阿伦森（Scott Aaronson）评述指出，近期多名前沿科研团队在代数复杂度核心猜想上取得重大突破，相继给出了瓦连特代数复杂度猜想中算术多项式与永久式不可互相有效归约

（即VP不等于VNP）的严格证明框架[43]。该突破被视为代数计算复杂性领域的里程碑，确立了经典算力与量子算力优势的坚实数学边界，将指引量子算法研究者避开已被证明无法超越经典优势的无效区域。此外，理论学者在《量子》期刊系统推导了高阶克利福德层次结构的群论映射法则，优化了通用容错计算中魔法态蒸馏的资源开销[15]；同刊另一论文推导出了针对多比特芯片失谐与串扰的最优校准模型，使多比特硬件标定测量步数减少了60%[13]；实验物理团队则成功在无壁势阱中捕获正电子并冷却至接近绝对零度，为检验微观粒子基本对称性奠定了基石[36]。

06 影响

今日影响



1 金融与政务核心密码防御体（受影响者）：RSA-2048破译逻辑资源首次降至10亿次托佛利门以内，同时美国国会山专家对长期数据泄密发出严重预警[3][22]。什么变了：原本留给金融系统与政务网络的抗量子密码迁移缓冲期被大幅缩短，算法升级从长远规划彻底转变为迫在眉睫的

合规防守红线。下一步值得盯什么：各国金融监管部门对商业银行核心系统后量子密码改造的合规时间表，以及硬件安全模块（HSM）的换代订单。

2 欧洲量子硬科技产业链（受影响者）：欧盟委员会正式发布配套500亿欧元主权科技股权基金的《量子法案》，欧洲量子产业联盟全面响应[27][45][49]。什么变了：欧洲本土量子硬件企业告别以往分散的科研经费拨款，迎来了全球规模最大的长期主权资本护航。下一步值得盯什么：首批主权科技股权基金在成员国间的认缴分摊，以及直接股权注资清单落地至本土整机企业的进展。

3 高端工业研发与仿真架构（受影响者）：罗尔斯·罗伊斯联手世外桃源和超威半导体在超算上跑通航发量子工作流，中国团队则凭经典超算仿真斩获戈登·贝尔奖[20][26]。什么变了：工业巨头对算力的规划全面转向「经典超算兜底、量子算法拔高」的异构混合求解路线。下一步值得盯什么：航空发动机燃烧室内流场模拟中，首个展现出超越纯经典数值计算经济性优势的工业实例。

4 容错量子硬件与系统工程（受影响者）：硅基自旋比特达成连续10天免校准稳定运行，马约拉纳拓扑物理比特迎来实验突破，同时QBlue编译器与QXL解码器大幅削减逻辑开销[19][23][24][35]。什么变了：底层硬件抗漂移周期的跃升与上层编译、解码工具的协同优化，使得全系统走向容错计算的工程复杂度显著降低。下一步值得盯什么：马约拉纳拓扑路线能否在2至3年内实现双比特编织门操作，以及专用解码硬件在商用测控机柜中的集成。

编辑点评

从今日多项进展的交汇点可以看出，量子计算正经历从单点硬件参数比拼向量子系统工程协同演进的关键拐点。一方面，上层算法与编译层展现出惊人的资源收敛速度，破译主流公钥加密所需的逻辑操作门槛被压缩至十亿次级别，配合形式化编译器高达九成以上的门数量削减，大幅降低了容错计算的理论算力门槛；另一方面，底层硬件正在摆脱以往频繁受制于电荷噪声漂移的脆弱状态，多天免校准稳定性的突破与实时纠错解码软件的介入，标志着量子硬件工程正在从实验室手工精调走向标准化自动化控制。这种算法下探与硬件上行的双向奔赴，正在让原本看似遥不可及的容错应用窗口加速重合。

与此同时，资本与产业落地层面的格局演变同样深刻。当主权政府开始以数百亿欧元规模的股权基金重塑产业链安全，当航空发动机巨头与跨国银行纷纷将量子算法内嵌至核心业务工作流，量子计算的商业逻辑已经完成了从纯科学探索向战略基础设施的定型。对于产业界而言，当下的核心任务已不再是无休止地争论何时实现完全容错，而是如何利用混合算力架构，在现有工程约束下率先攻克经典超级计算机无法触及的局部工业瓶颈。在这场持久战中，谁能率先打通从芯片校准、编译优化到特定垂直行业软件的完整链路，谁就将在真正的量子算力时代到来前锁定最坚固的生态护城河。

参考资料

[1] Genesis Mission assembles Avengers to accelerate American science

[2] Early-Stage Prototype Products in Quantum Chemistry and Quantum Life Sciences

[3] Experts Urge Federal Agencies to Move Faster on Quantum Defenses

[4] Regional attention transformers for spatially structured open quantum dynamics

[5] Quantum ingenuity can sidestep limits of conventional chips—while using commercially accessible components

[6] New quantum network entangles 123 qubits that store information in atoms' positions

[7] Quantum leap: Computing's next frontier takes shape

[8] DNA-based quantum sensors could improve bioimaging

[9] Research Scientist (Theory) Online Decoders

[10] Monthly Seminar: Carleman Lattice Boltzmann for turbulent flows

[11] Distributed Quantum Computing on Networked Trapped-Ion Systems (IonQ and UofT)

[12] Postdoctoral Positions in Multipartite Entanglement and Quantum Communication

[13] Optimal Calibration of Qubit Detuning and Crosstalk

[14] Quantum fields in a cold atomic simulator: relaxation and phase locking in tunnel-coupled 1D bosonic quasi-condensates

[15] Climbing the Clifford Hierarchy

[16] Logarithmic-depth quantum state preparation of polynomials

[17] Recursive Clifford noise reduction

[18] IonQ to deploy a 256-qubit computer at Cambridge by summer 2027

[19] Verified compiler cuts gate count for quantum simulations by 94%

[20] AMD′s Lux supercomputer runs Xanadu′s largest quantum workflow

[21] Polarization-entangled photons generated at a rate of over 4 million pairs per second

[22] Fewer than one billion Toffoli gates now needed for RSA-2048 factoring

[23] Spin qubits maintain rotation angle to 0.3 degrees for ten days

[24] QXL cuts decoder errors by 13% on Google hardware

[25] Tsinghua University achieves 546Hz atom-to-atom entanglement over city fibres.

[26] Quantum leap for Chinese team’ s exascale chemistry simulation wins Bell Prize

[27] European Commission Proposes Quantum Act and New Sovereign Tech Equity Fund

[28] Schism architecture achieves up to 4.9-7.3x speedup on 32 quantum processors

[29] Foliated codes suppress leakage errors by 1380 per two rounds

[30] Nexent Capital IFSC Launches $1 Billion Quantum Computing-ready AI Infrastructure & Advanced Energy Fund

[31] QlayBot agent designs quantum devices from images with 81.5% success

[32] Neutral atoms simulate complex materials with quantum-classical hybrid method

[33] Hyperentangled photons aid quantum key distribution

[34] Quantum Walton Institute explains quantum technology on national Irish television

[35] QuTech demonstrates a qubit based on Majorana quasiparticles

[36] Physicists trap antimatter in a breakthrough that could explain why the universe exists

[37] In 2022 NASA struck an asteroid. Now we are finally seeing the massive impact up close

[38] The U.S. Army is blowing up five tons of toxic lead azide in Iowa

[39] How the Galileo musical’ s composer sets science to a score on Broadway

[40] A new biography reveals the private life of Stephen Hawking

[41] This is the best time to eat Thanksgiving dinner for your health

[42] Do you need to be worried about flying for Thanksgiving this year? We asked the experts

[43] HOLY SHIT HOLY SHIT HOLY SHIT HOLY SHIT

[44] IQM to Deploy 54-Qubit Quantum Computer at South Korean Data Centre

[45] QuIC Welcomes the European Quantum Act, Pledges to ‘Mobilize Industry’

[46] Guest Post: After DeepMind’ s RSA Results, The Case For QKD on Critical Links

[47] Chulalongkorn Researchers Call for Greater Quantum Investment in Thailand

[48] Standard Chartered Expands Quantum Computing Research Program Following Successful Research Phase

[49] The Qubit Report for November 25, 2026: Europe’s €50B Fund, IQM Korea Order, TUM Humboldt

量子研究内参

全部期数 · 周刊深度解析 · 每日快报 → qbitbrief.com

FOR RESEARCH REFERENCE ONLY

配图源自所引论文与新闻稿；如引用不规范，请联系编辑部删除。